IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Art Unit	:	
Examiner	:	
Serial No.	:	**Customer No. 035811**
Filed	: Herewith	
Inventor	: Michael Arnouse	
Title	: SYSTEM AND METHOD OF : FOR NETWORK SECURITY	Docket No.: 1221-CIP-03
		Dated: August 22, 2003

PETITION TO MAKE SPECIAL
UNDER 37 C.F.R. § 1.102(d)
INVENTIONS FOR COUNTERING TERRORISM

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby petitions under 37 CFR § 1.102(d) and MPEP 708.02(XI) that the subject application be accorded special status and advanced in order of examination on the basis of inventions for countering terrorism.

The requirements of 37 CFR § 1.102(d) and MPEP 708.02(XI) are fulfilled as follows:

1. A check for the appropriate fee $130.00 as set forth in 37 C.F.R. §1.17(h) is attached hereto.

2. The patent application presents Claims 1-43 drawn to a single invention. In the event that restriction is required, an election will be made without traverse.

3. An Information Disclosure Statement (IDS) is filed concurrently herewith. The listed publications, copies enclosed, represent the results of the search.

4. A statement explaining how the invention contributes to countering terrorism follows.

08/27/2003 MAHMED1 00000063 10647080
01 FC:1460 130.00 OP

The following describes one exemplary embodiment in relation to homeland security. In this embodiment, a foreign national enters the United States(or similarly, some other country) and is issued an identification memory card. The card may be encrypted with a digital photograph and other unique identifying biometric data, such as a fingerprint. The entry is permanently time, date and place stamped by indisputable GPS chip in the card. This card can be tracked in real time or traced with each use. Uses in cards for student visas, visitor visas, passports, etc., can be utilized with this technology. The legal record for this individual can be entered into the card, such as the purpose here in the U.S. and who the immediate family members are, etc. This information may be seen only by the proper legal authorities, such as the police, INS, etc. No one else can use the individual's card because of the biometric utilization features. Without the fingerprint, for example, the card is useless and cannot be read. An individual is linked to a particular card. The card may also be tracked where desired. If someone is being sought for illegal activity, as an example, the card will locate them via GPS. If they have discarded the card and are apprehended with someone else's card, the biometrics will not match. If they do not have any card, or a proper card, then their biometric data will reveal their true identity. Law enforcement will have biometric readers that are part of the system to help in this process.

Furthermore, in other embodiments, cards may be utilized as a social security/homeland security card. These cards can provide accurate information that preferably cannot be altered with the exception of authorized government agencies that issue the data. The biometric link to each card verifies the individual of the card as owner and can place the owner at a specific location, date and time. This system provides an unprecedented level of personal identity security and protects society from imposters and criminals wishing to cause harm by using deceitful practices. The social security

number for each person can be digitally encrypted and protected by multiple levels of biometric security. This will virtually "identity theft proof" the card. Individuals may also choose if they want the card to be trackable in real time to help them locate it if lost. The universal applications will encourage people to want to have a single memory card as opposed to a wallet full of separate conventional cards.

In one exemplary embodiment, where an electronic communication may be desired to be sent from one computer to another computer, a biometric security measure may either be packaged with or sent associated with the electronic communication (i.e, substantially at the same time or before/after) and received by a server. A biometric comparison is then conducted at the server, such as fingerprints mentioned above, although as should be understood, any other biometric information may also be used as well. Based on the biometric comparison and/or presence/absence of any other data stored in the database, the electronic communication may either be routed to the destination computer, if authorized, or routed to some other destination or retained at the server, if not authorized.

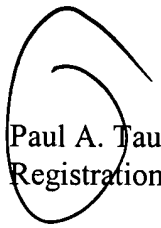
Further, the server may also be utilized to detect the presence of any viruses, worms, etc associated with the communication, and then similarly route any problem communication to designated locations other than the destination computer or retained at the server. In addition, where any problem is detected, the sender's biometric information may be forwarded to authorities where desired for identification purposes.

The foregoing system may be utilized where ever desired, and in particular, where ever network security may be a concern, such as, for example, any government agencies, financial institutions, databases containing any sensitive company or personal information, etc.

Applicants respectfully submit that all requirements called for by the applicable rules have been fulfilled. Applicants respectfully request early favorable action on this Petition.

Accordingly, Applicants respectfully request that the Petition to Make Special be granted, and that the application be taken out of turn for examination. Applicants also respectfully request an early consideration and allowance of the solicited claims.

Respectfully submitted,



Paul A. Taufer
Registration No. 35,703

PAT:ers
(215) 656-3000